By John Leyden, TheRegister.co.uk

A Russian security firm has pledged to release details of previously undisclosed flaws in enterprise applications it has discovered every day for the remainder of January.

Intevydis intends to publish advisories on zero-day vulnerabilities in products such as Zeus Web Server, MySQL, Lotus Domino and Informix and Novell eDirectory between 11 January and 1 February, security blogger Brian Krebs reports.

As an opener, Intevydis published a crash bug in Sun Directory Server 7.0, along with exploit code. The final line-up of zero-days is still being finalised, but the MySQL buffer overflows and IBM DB2 root vulnerability flaws on the provisional menu sound much tastier than Intevydis`s somewhat bland opener. Advisories are due to be published on the Intevydis blog here .

Intevydis said it launched its campaign after becoming more and more disillusioned with foot-dragging by vendors when confronted by security flaws in their products. ˝After working with the vendors long enough, we've come to conclusion that, to put it simply, it is a waste of time,˝ Evgeny Legerov, a founder of Intevydis told Krebs. ˝Now, we do not contact with vendors and do not support so-called 'responsible disclosure' policy.˝

Only one software vendor, Zeus, reportedly worked with Intevydis in developing a patch to be released at the same time as an upcoming advisory from the Russian security firm. Intevydis`s stance is likely to reboot the long running debate about the responsible disclosure of security vulnerabilities.

An entry on the Intevydis blog accuses software vendors of exploiting researchers as unpaid lackeys.

During the time our position to responsible disclosure policy has been evolved and now we do not support it. Because it is enforced by vendors and it allows vendors to exploit security researches to do QA work for free.

The Russian firm intends to publish exploit packs covering the vulnerabilities it covers that hook into Immunity`s Canvas penetration testing tool. Immunity does not routinely notify affected vendors about vulnerabilities covered by its tool, in contrast to other programs that also make use of vulnerabilities discovered by security researchers.

For example, TippingPoint's Zero-Day Initiative and Verisign's iDefense Vulnerability Contributor Program pay security researchers for discovering exploits while also notifying vendors that something is amiss. The two firms liaise with vendors on developing fixes while discreetly adding updates to their products designed to prevent unpatched vulnerabilitiess from causing any harm.

Intevydis said it has made money from both the ZDI and iDefense programs in the past, but has now decided to go further with what might come across as a name-and-shame scheme designed to push vendors into developing security fixes more quickly.